

h

Notice of Allowability

Application No.

09/690,110

Applicant(s)

MURTHY ET AL.

Examiner

Art Unit

Grigory Gurshman

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to Appeal Brief filed on 7/20/2005.
2. ☒ The allowed claim(s) is/are 1-21.
3. ☒ The drawings filed on 16 October 2000 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|---|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____ |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____ |

DETAILED ACTION
EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Steven T. McDonald on 8/16/2005. The amendment is made in order to correct a single means claim.

2. The application has been amended as follows:

In specification: on page 18, line 4 replace "**components**" with "**means**".

Claim 17: A system for providing at least one independent auditor an audit trail, the audit trail having one or more records recording actions taken against a database, the integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditor, the database having a writing machine (writer) not under the control of the access-privileged user or the auditor, the system comprising ~~means for~~:

means for integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor,

means for ~~wherein the writer has an~~ to have access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key),

wherein only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key), and
means forwherein the auditor to be able ~~has the ability~~ to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user.

Allowable Subject Matter

3. Claims 1-21 are allowed.
4. The following is an examiner's statement of reasons for allowance:
 - 4.1 Referring to claims 1-21, Strickler discloses database replication scheme (see abstract and Fig.2). Strickler teaches the system having a plurality of nodes connected via communication media in a topology. Each node includes a database and a transaction transmitter or collector, which sends transactions posted to the database to a database at one or more other nodes for replication in the databases of the one or more other nodes. All transactions to be posted to databases in remote nodes that were sent by a local node are detected (see abstract). Strickler teaches that as applications 12 make modifications (e.g., inserts, updates and deletes) to the data in the audited source database 14, TMF (transaction monitoring facility) or TM/MP (transaction monitoring/massively parallel) records the details of the transactions in audit trail files 18. A shadowbase object or process, known as a "collector" (collector 20) reads the

audit trails in the audit trail files 18 and collects changes made to the source database 14 (see Fig.2 and column 2, lines 48-55).

Strickler, however, does not teach or suggest a method of *initiating the audit trail by generating an initial value of an authentication token and an initial value of a validation token*. Strickler generally describes an audit token, but neither describes or suggests *generating an initial authentication token and an initial validation token for the audit trail*.

Furthermore, Strickler does not teach or suggest that the tokens are based *on a first encryption key of a first type (writer public key) generated by the writer and a second encryption key of the first type generated by each Auditor (auditor public key)*.

4.2 Referring to the instant claims, Cordery discloses a method of token verification (see abstract). Cordery teaches that computer (24 in Fig.) records a local time for an audit trail. Cordery also teaches that encryption is performed using a cryptographic key. In each digital meter, independent keys are used for generating the digital tokens.

For security reasons, the keys in different meters are also independent. Information about the meter and mail piece are combined and encrypted with vendor and postal master keys or keys derived therefrom. Portions of the resulting information are printed on the mail piece as digital tokens. The information and tokens can be verified by a device that processes the information in the same manner and compares the resulting digital tokens with those printed on the mail piece (see column 2, lines 7-20).

Cordery, however, does not teach or suggest that the tokens are based *on a first encryption key of a first type (writer public key) generated by the writer and a second encryption key of the first type generated by each Auditor (auditor public key)*.

4.3 Therefore, the combination of Strickler with Cordery does not render the instant claims obvious. In view of the reasons presented herein, claims 1-21 are in condition

for allowance.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

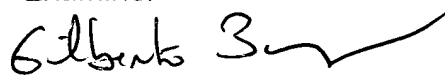
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

GB.

Grigory Gurshman
Examiner



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100